CompTIA A+ 11.0 Networking

11.6.2 SOHO Configuration Facts

Many networks today fall into the category of a small office/home office (SOHO) network. A SOHO network is a smaller network that does not use servers to manage network resources or enterprise level switches to connect devices. Most wireless networks used in homes are considered SOHO networks.

This lesson covers the following topics:

- SOHO wireless router
- Wireless router configuration
- Wireless network configuration

SOHO Wireless Router

Typically, a SOHO network consists of a single router connected to the internet. These wireless routers are often all-in-one devices that contain the following functions:

- Router – Connects the internal network to the internet.
- Switch – Connects internal devices together using RJ-45 connections.
- Wireless access point – Provides access to the wireless connection.
- Modem – If the ISP supplies the wireless router, the modem functions are built into the wireless router.

When choosing a wireless router, consider the following:

- Appropriate 802.11 standard – The router should support the same standard as the client devices. The 802.11 standard also determines the transfer rate of connected devices.
- Transmit power – The router should be powerful enough to transmit to all needed areas in the building. Wireless extenders might also be needed for larger areas.
- Special features – Many wireless routers have additional features that are designed to improve performance. These features are typically unique to each manufacturer.

Wireless Router Configuration

Before you can configure the wireless network, perform the following initial steps to configure the wireless router.

Wireless Router Configuration	Description
Change default username and password	Wireless routers are shipped with a default username and password. This default login information is readily available on the internet, so change it before you do anything else. Always use a strong password. You cannot change the default username on all routers, but you can always change the password.
Update firmware	Often a firmware update is available, even for new routers. Firmware updates address bugs, security vulnerabilities, and may add new features. Always keep the firmware up to date.
Physically place the router	When physically placing the wireless router, ensure that all areas have needed coverage. Each building is unique and placement depends on a variety of factors including size, building materials, and other wireless devices that might cause conflicts. Anyone with physical access to the router can make configuration changes and gain access to the network. To prevent this, limit physical access to the router. For example, place the router and other networking equipment in a locked closet.

Wireless Network Configuration

The first step in configuring the wireless network is to connect the wireless router to the internet modem. The modem connects to the router port that is typically labeled Internet or WAN. Once the router is physically connected, configure it to connect to the internet. The configuration options depend on the type of internet service. Typical options include:

- DHCP – This is the most common configuration option. Using DHCP, the router contacts the ISP to obtain the connection information including the IP address, subnet mask, and DNS server.
- Static – Some internet providers provide users with a static configuration. This means that you must manually configure the IP address, subnet mask, and DNS server.
- Point-to-Point Protocol over Ethernet (PPPoE) – PPPoE is a protocol typically used by DSL providers that allows them to regulate internet access using username and password authentication.

Once you configure the internet connection, you can configure the wireless network. The following table describes many of the settings that you might have to configure.

Wireless Network Configuration	**Description**
Service Set Identifier (SSID)	The SSID is the unique name for the wireless network. Wireless routers have a default SSID that should be changed. Keep the following in mind when setting the SSID: • The name cannot be the same as any other network in the area. • The SSID has a maximum length of 32 characters. • SSIDs are case sensitive. • The SSID should not contain any personal or identifiable information. • Special characters (spaces, dashes, periods, etc.) are allowed, but can cause issues with some connecting devices. It is best not to use special characters. *SSID suppression* (cloaking) disables the SSID broadcast. With broadcasting disabled, the user must manually enter the SSID for a device to connect to the network. This means the SSID doesn't display in the list of available networks). Even with the broadcast disabled, it's relatively easy to identify the SSID of a network by using readily available applications. Because of this, SSID suppression should not be the only form of protection.
Configure the wireless protocol	Many access points support multiple wireless protocols. Configure the wireless router to use only the protocols needed for devices on the network. When using mixed mode (more than one protocol), most access points throttle all clients to the slowest protocol speeds being used.
Configure the wireless channel	The channel identifies the portion of the wireless frequency the access point and connected devices use. • Select a channel that does not conflict with other access points or devices in the area. • Many access points have an automatic channel feature that detects other access points and automatically selects the channel with the least amount of traffic.

Wireless Network Configuration	**Description**
Authentication and encryption	Authentication allows only authorized devices to connect. Encryption protects wireless communications from eavesdropping. • Most SOHO networks use WPA2 or WPA3. • For WPA2, use a strong shared secret (passphrase). • Use WPA3 if all devices on the network support it.
Disable guest access	Guest access allows anyone to access the network connection, but be sure to configure it to restrict access to the internal network. Disable guest access unless the wireless network is configured for public access.
Network Address Translation (NAT)	Small networks use a single public IP address to connect to the internet. All devices on the private network share this IP address. Network address translation (NAT) is a protocol that allows multiple computers to share a single public IP address on the internet. • The internet is classified as a public network. All devices on the public network must have a registered IP address. This address is assigned by the ISP and is used by the WAN port on the wireless router. • A SOHO network is classified as a private network. All devices on the private network use private IP addresses internally, but share the public IP address when accessing the internet. • The private network can use addresses in the following ranges that have been reserved for private use (i.e., they will not be used by hosts on the internet). o 10.0.0.0 - 10.255.255.255 o 172.16.0.0 - 172.31.255.255 o 192.168.0.0 - 192.168.255.255 • A NAT router associates a port number with each private IP address. Communications with the private hosts from the internet are sent to the public IP address and the associated port number. Port assignments are made automatically by the NAT router.
Security settings	Security settings you might need to configure include:

Wireless Network Configuration	Description
	• A basic firewall on the router provides an additional level of security for the private network. o Any unused ports should be closed to prevent a potential attacker from gaining access through an open port. o If necessary, configure exceptions to allow specific traffic through the firewall. • Some applications use specific ports for traffic. o You can configure port forwarding to allow any traffic coming in on the specified port(s) to be routed to a specific IP address of an internal device. o You should enable port forwarding only when transferring data. To help keep the network secure, disable port forwarding when it is not in use. • Some networks might have a resource (such as a web server) that is open to external users. o You should enable and configure a screened subnet (previously referred to as the demilitarized zone or DMZ) for resources open to external users. o Configuring a screened subnet on a SOHO router causes all incoming port traffic to be forwarded to the specified screened subnet host. o Because this can open the network to a variety of external threats, use the screened subnet only when necessary. • Content filtering – Most SOHO routers provide content filtering and parental controls that prevent hosts from accessing specific websites or using a specific internet service, such as chat, torrent, or gaming applications. • IP filtering – You can configure the router to explicitly allow or deny specific IP addresses access to the network. • MAC address filtering - You can configure the router to explicitly allow or deny specific MAC addresses to connect to the network. This is considered a very weak form of security and should not be used.

Wireless Network Configuration	**Description**
Universal Plug and Play (UPnP)	UPnP allows devices like printers, webcams, gaming consoles, and similar devices to discover devices and automatically connect. • You can configure these devices to automatically open needed ports to allow connections to the internet as needed. • While this does make using these devices much easier, it is a security concern since these devices can accidentally create a hole in the wireless networks. • If this service is not needed, disable it to help keep the network safe.
Quality of Service (QoS)	Most SOHO routers provide basic QoS functionality. When enabled, QoS prioritizes certain network communications over others. For example, VoIP network traffic is given higher priority and more bandwidth than HTTP (web browser) traffic.
Wi-Fi Protected Setup (WPS)	The WPS security protocol makes it easier for WPS-enabled devices (e.g., a wireless printer) to connect to the wireless network. • WPS can use several methods for connecting devices, including the PIN method and the push button method. • Both the access point and the wireless device must support the method used to connect devices.

Every network is unique and requires a different configuration. You will not use the same options for every network.